2003년도 대한전자공학회 하계종합학술대회 논문집 제26권 제1호

ISP 망의 취약성 및 보안 이슈

이승민, 남택용, 손승원
한국전자통신연구원 네트워크보안연구부

ISP Network's Vulnerabilities and Security Issues

Seungmin Lee, Taekyong Nam, Seungwon Sohn
Network Security Research Department
Electronics and Telecommunications Research Institute
E-mail : todtom@etri.re.kr

Abstract

최근의 인터넷을 통한 사이버 공격 유형은 시스템 위주의 공격에서 네트워크 공격으로 변화하고 있다. 이에 따라 망을 소유하고 인터넷 서비스를 제공하는 ISP 관점의 보안이 중요한 변수로 등장하기 시작하였다. 본 논문에서는 1.25 인터넷 대란과 같은 국가차원의 사태 재발 방지를 위하여 현재 인터넷망의 취약성을 분석하고 이에 대한 보안 해결책으로서 보안 시스템의 성능, 기능 관점의 보안 이슈와 서비스 관점에서 보안 요구사항을 살펴보았다. 또한 이를 종합하여 네트워크 영역 관점에서 앞으로 중점적으로 다뤄야 할 보안 연구 분야를 제시하였다.

I. 서론

정보화 사회의 도래와 더불어 다양한 사이버 범죄가 등장하여 개인의 사생활 침해나 경제적 손실은 물론이고 국가 안보와 사회질서를 위협하는 사례까지 발생해 왔음은 잘 알려진 사실이다. 더구나 최근의 1.25 인터넷 대란과 같은 사건은 국가 전반에 걸쳐서 영향을 끼친 대표적인 사례라고 볼 수 있다.

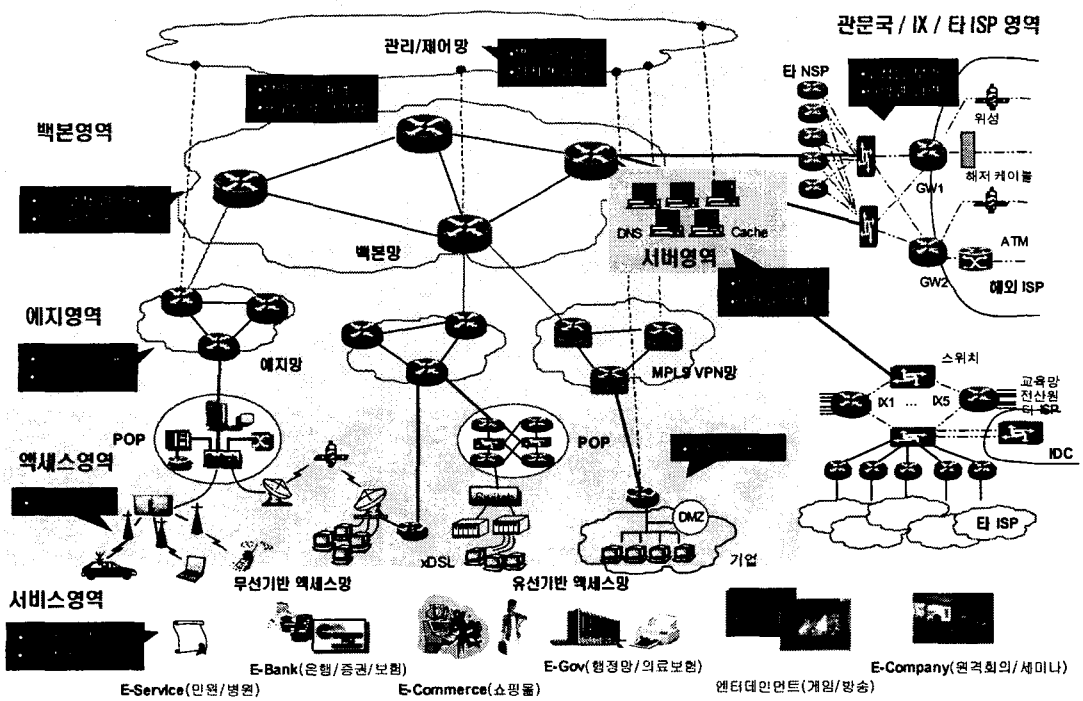
국가의 중요한 서비스와 인프라를 제공하는 ISP 입장에서 볼 때, 해킹이나 바이러스 등으로부터 정보의 파괴와 왜곡을 막는 기존의 시스템 보안 기술은 많은 한계점을 드러내기 시작하였다. 즉, 점점 사이버 공격의 형태가 시스템 위주의 공격에서 네트워크 공격으로 변화하고 있기 때문이다.

최근 1.25 인터넷대란을 계기로 국내 인터넷 사업자들은 제2의 인터넷 대란을 대비하기 위해 네트워크 보안성 강화에 많은 노력을 기하고 있다. KT, 데이콤, 하나로, 온세, 두루넷 등의 ISP들은 악성 웜바이러스 공격을 효과적으로 차단할 수 있는 L7 스위치 기반의 침입방지시스템을 설치하는 한편 비상대책반을 운영하고 있는 실정이다. 이러한 인터넷 대란은 사이버 공격의 형태가 시스템 위주의 공격에서 네트워크 공격으로 변화하고 있음을 단적으로 보여주고 있다. 이는 ISP에서 제공하는 보안 서비스를 선택하는 결정적인 변수로 등장하게 되면서 네트워크 기반의 보안 서비스의 중요성을 증가시키고 있다.

본 논문은 국가차원의 인터넷 마비 사태를 방지하고, 안전하고 신뢰적인 인터넷 서비스를 제공하기 위하여, ISP 입장에서 바라본 망의 취약성을 분석하고, 이에 대한 해결책으로서의 보안 이슈를 제시하였다.

II. ISP 망의 취약성

본 절에서는 ISP 관점에서 영역별 인터넷망을 살펴보고 이에 따른 취약성을 분석하기로 한다. [그림 1]은 ISP 을 구성하는 인터넷과 취약성을 나타낸 것이다.



[그림 1] ISP 망의 취약성

2.1 백본영역

◈ 성능 보장형의 하드웨어 기반 라우터 부재로 인한 ISP 망의 구조적인 병목현상을 유발

◈ 라우터 및 스위치 단에서 멀티캐스트 패킷에 대한 drop 기능 미 설정과 IP 주소 위조 패킷 등 유해 트래픽을 차단할 수 있는 블랙홀(black hole) 및 싱크홀(sink hole) 필터링 기능을 탑재한 네트워크 장비 미흡 등의 보안 관리 메커니즘 부재

◈ 보안관리 전문가 부족, 신속한 대응 및 분석 체계 미흡, 유기적 연동 및 체계적인 유지관리 등의 보안관리 체계 미흡◈ 인터넷 프로토콜(예:BGP)의 취약성을 이용한 다양한 공격 가능성

◈ 라우터의 로그기록 등을 이용한 공격자에 대한 실질적인 역추적 방안 부재

◈ 네트워크 노드와 관리시스템간 또는 관리시스템간의 통신 방식이 별도의 전달통로가 없는 in-band 방식을 채택하고 있음. 따라서, 트래픽 폭주시 경보 및 제어 신호의 전달이 불가능함

◈ 내부 관리자에 의한 관리시스템으로의 접근은 대부분의 경우 무방비 상태에 놓여 있는 취약성 존재

◈ 실시간 감시 및 조기경보 기능 부재

2.2 서버영역

◈ 서버 자체(OS, application 등)에 존재하는 취약성

◈ DNS 서버, DHCP 서버 등 중요 정보통신 인프라의 안전한 구조로의 설계 및 가용성 확보 미흡 (설비 용량 증설, 분산 설치, 백업 체계 구축 등)

2.3 에지영역

◈ 에지 라우터의 접속 구조 분산화 및 네트워크 장비의 보안기능 미흡

◈ 수용 트래픽량을 고려한 라우터 용량의 증설 및 망 구조의 분산화 미흡

◈ 스위치 및 라우터 단에서 IP 주소 위조 패킷 등 유해 트래픽을 차단할 수 있는 기능 미흡

◈ 네트워크 장비에 대한 관리용 포트를 이용한 원격접속(Telnet, FTP, Rlogin 등)을 이용한 해킹 가능성

◈ 서비스의 연속성을 방해하는 신속한 복구 방안 취약

◈ 외부 침입에 독립적인 지속적인 기능개선으로 시스템의 내성을 강화할 수 있는 방안 부재

2.4 액세스영역

◈ 무선 단말의 보안 취약
◈ 무선 인터넷 서버의 취약
◈ 무선 방송의 컨텐츠 보안 취약
◈ xDSL 가입자 수용을 위한 스위치 또는 라우터의 용량 증설, 과다 유입 트래픽의 분산 등 망 접속 구조를 개선하고 보강할 수 있는 방안 미흡
◈ ISP 와 협약으로 신속한 보안기능 제공방안 부재

2.5 서비스영역

◈ 사용자의 요구 수준에 따라, 사용자가 원하는 서비스를 안전하고 신뢰적으로 보장할 수 있는 보안기술 부재
◈ Multi-dimensional 서비스 트랜잭션의 시작과 완료 시까지 세션의 안전한 유지 관리 미흡

2.6 관문국/IX/타 ISP 영역

◈ 인터넷 기간망 처리 능력은 최고 수십 Gbps 임에 반해, 현재의 정보보호 제품의 처리 능력은 최고 수백 Mbps 급에 불과하여 실제 망에 적용하는 데 어려움이 있음
◈ 타 ISP, NSP 와 취약성 정보 및 외부 침입 정보 등에 대한 공유가 되지 않음
◈ 역추적이나 패킷 차단 등의 대응 방안 시, 타 ISP 및 NSP 와의 협력체계가 없음

III. 취약성에 대한 ISP 보안 이슈

본 절에서는 앞서 살펴본 인터넷의 보안 취약성을 해결하기 위한 ISP 관점의 보안 이슈에 대하여 살펴 보기로 한다. 먼저, 현재 인터넷 대역폭의 증가에 따른 주요 백본 라우터의 성능을 통하여 보안 시스템에 요구되는 성능을 추측해 보고, 네트워크 보안 시스템의 기능 관점의 요구 변화를 통하여 향후 보안 이슈로 등장할 correction 기술의 필요성을 살펴 보기로 한다. 그리고 서비스 관점에서 가입자에게 요구될 서비스의 주요 특징들을 짚어보기로 한다. 마지막으로 지금껏 살펴본 취약성에 대한 해결방안을 영역관점에서 정리한 후, 이를 통하여 향후 보안 기술과 연구 영역을 확인하기로 한다.

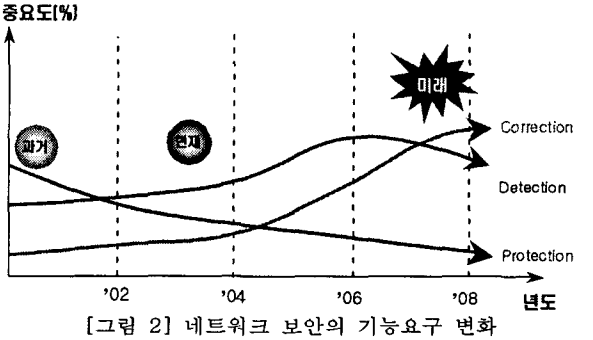
3.1 성능 관점의 보안

[표 1]은 년도별 인터넷백본망의 대역폭 증가에 따른 주요 백본 라우터의 성능 예측치이다. 이에 따라 ISP 입장에서는 백본망영역의 성능보장형 보안 스템의 필요성이 점점 증가하고 있다.

[표 1] 인터넷 대역폭과 백본 라우터의 성능 예측

년도	백본망 대역폭	세계 주요 백본 라우터	
		line rate	throughput rate
2002	10Gbps	2.5Gbps 이상	1Gbps
2004	40Gbps	20Gbps 이상	1Gbps 이상
2006	160Gbps	80Gbps 이상	2Gbps 이상

3.2 기능 관점의 보안

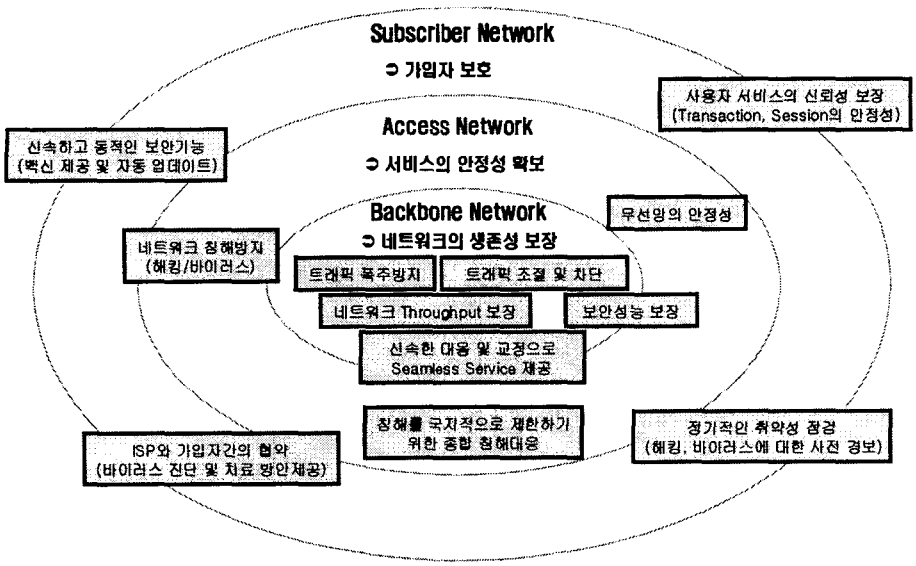


[그림 2] 네트워크 보안의 기능요구 변화

인터넷 보안에 대한 기능 관점의 대응 변화는 [그림 2]와 같이 과거에는 외부 공격이나 침입에 대한 방어(예:방화벽) 위주의 네트워크 보안이었다면, 현재는 탐지 및 대응(예:침입탐지시스템)을 통한 네트워크 보안이 주를 이룬다고 볼 수 있다. 그러나 향후에는 신속하고 신뢰적인 교정이 가능한 보안 제어 기술이 중요한 이슈로 등장할 것이다. 이러한 교정기술은 안정적이고 신뢰적인 네트워크를 보장하여 seamless service 를 제공할 수 있다.

3.3 서비스 관점의 보안

인터넷 이용자의 급증과 함께 바이러스, 해킹으로 인한 네트워크 침해 사고의 확산으로 서비스에 대한 보안기술의 필요성과 중요성이 증가하고 있으며, 나아가서 책임성 또한 커지고 있다. 그러나 현재의 보안기술은 시스템, 네트워크 수준에서 대응하는 데 그쳐, 안전하고 신뢰성 있는 인터넷 서비스를 제공하는 데 어려움이 있다. 따라서 향후에는 보안이 요구되는 mission-critical 서비스에 속하는 사용자 트랜잭션의 안전한 수행과 완료를 보장하기 위해 가변적인 대역폭 할당 및 안전한 다중 경로 제공 기술이 가입자측면의 가장 큰 요구사항으로 등장할 것이다.



[그림 3] 네트워크 영역관점의 보안 이슈

가장 큰 요구사항으로 등장할 것이다.

3.4 네트워크 영역 관점의 보안

지금까지 바라 본 성능, 기능, 서비스 관점을 포함하여 취약성에 대한 해결방안으로서 네트워크 영역관점에서 이를 분류, 정리해 보기로 한다. [그림 3]은 이를 나타낸 것으로 크게 에지영역과 관문국영역 등을 포함한 백본망과, 액세스망, 그리고 서비스영역을 포함한 가입자망으로 구분하여 각각에서 요구되는 솔루션을 제시하였다.

백본망의 경우, 네트워크의 생존성 보장이 가장 핵심적인 보안 이슈이며, 이를 위하여 DDoS 등으로부터 트래픽 폭주 방지, 트래픽 조절 및 차단, 그리고 네트워크의 대역폭 보장 등을 들 수 있다. 그리고 외부 침입에 대한 신속한 대응 및 교정과 성능 보장 보안 제품 개발이 또 하나의 보안 이슈로 고려해야 한다.

액세스망의 경우, 가입자의 서비스를 백본망에 안전하게 전달하여 서비스의 안정성 확보를 가장 중요한 이슈로 들 수 있으며, 이를 위하여 해킹과 바이러스 등으로부터 네트워크 침해를 방지하고, 국지적으로 침해를 제한하기 위한 대응책이 요구된다. 그리고 무선가입자의 증가에 따른 무선망에 대한 보호가 또 하나의 새로운 연구 분야로 볼 수 있다.

서비스영역이 존재하는 가입자망의 경우, 점점 사용자 서비스에 대한 신뢰성을 보장하는 것이 가장 중요한 보안 이슈로 등장하게 될 것으로 보인다. 이는 유무선 통합과 음성과 데이터의 통합으로 서비스 융합이 본격화 되는 시점에서 가장 핵심적인 요구 사항이 될 것이다.

IV. 결론

본 논문에서는 현재 보안 분야에서 가장 큰 이슈로 등장하고 있는 ISP 망의 보안을 해결하기 위하여, 인터넷망의 영역별 취약성 분석을 통하여 다양한 관점의 보안 이슈를 정리하였다. 이는 공중망이나 증권, 은행, 보험 업계의 전산망 뿐만 아니라, 국방망, 행정전산망과 같은 국가의 중요 네트워크에 적용 되어 신뢰성 있는 인터넷과 서비스 환경을 구축하는 데 핵심적인 역할을 할 수 있을 것으로 기대된다.

참고문헌

[1] J.Pescatrore, M. Easley, R.Stiennon, " Network security platform will transform security markets" , Gartner, Nov. 2002.

[2] " State of the NGN : Carrires and Vendors must take security seriously" , Gartner, March. 2003.

[3] 네워크 기반 정보보호체계 구축 계획(안), 정보통신부, 2003.2.